REMARKS

Claims 1-3, 5-7, 9, 12-29, 31-32, 35-38, and 40-44 are pending. Applicant requests that Claims 1, 5, 25, 32, 38, and 44 be amended to place the application in form for allowance or better form for appeal. Claims 4 and 10-11 have been canceled. No new matter has been added. The rejections of the claims are respectfully traversed in light of the amendments and following remarks and reconsideration is requested.

Rejection Under 35 U.S.C. § 103

Claims 1-7, 9-17, 19-29, 31-32, 35-38, 40-44, and 46-48 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Sims, III (U.S. Patent No. 6,550,011 hereinafter "Sims") in view of Abbott et al. (U.S. Patent No. 6,671,808 hereinafter "Abbott").

In rejecting the claims, the Examiner writes in part:

> In respect to claim 1, Sims discloses . . . a user program running on the processing device, the user program configured to control access to the rights controlled data object; a user program security module configured to at least partially decrypt the secure package using a user program key associated with the user program (see col.9, lines 60-67).

However, Sims discloses the following:

> According to a volume or super distribution model, where large quantities of content are distributed . . . content would preferably be encrypted once and everybody utilizing the same content would require the same content key in order to decrypt that content.
>
> Additionally or alternatively, it is also possible to uniquely encrypt the content per user so that if unauthorized copies are made available or a secret key is published the source might be identified. However, use of multiple content keys for a single protected work increases costs in that multiple keys must be generated and maintained as well as multiple pr[o]cessing of the content to encrypt it must be accomplished. (Sims, col.9, lines 60-67) (emphasis added).
>
> [T]he information use device is preferably adapted to associate each content key with its corresponding content. (Sims, col.11, lines 30-32).

Thus, Sims discloses a content key associated with content and a user but not a user program key associated with the user program. Abbott is directed toward a "USB-compliant personal key" and does not remedy the above-noted deficiency of Sims. Applicant could not locate any disclosure in either Sims or Abbott related to a key associated with the user program and used for decryption. Accordingly, Sims in view of Abbott does not disclose or suggest the use of multiple levels of encryption/decryption with keys associated with the user program, the user, and the processing device.

In contrast, the present disclosure teaches the following:

> The first security module 352 uses a first key (the user program key) 115 for some or all of its security functions.
>
> The first security module 352 . . . allows functionality of the second and third security modules 354, 356 to be disabled while still maintaining the ability to communicate secure packages. This feature allows a data object 106 to be used in conjunction with the system even when the data object provider does not want to restrict the use of the data object 106 to a particular user or data processor 300. (Publication No. US2001/0029581, paragraphs [0057]-[0058]).

In particular, amended Claim 1 recites a data processor, comprising "a user program security module configured to at least partially decrypt a first secure layer of the secure package using a user program key associated with the user program; a user key device associated with a user, the user key device detachably connected to the processing device, accessible by the user program, and configured to restrict the use of the data object to the user using a user key for decrypting a second secure layer of the secure package; and a machine key device connected to and associated with the processing device and accessible by the user program, the machine key device configured to restrict the use of the data object to the user data processor using a machine key for decrypting a third secure layer of the secure package."

Similarly, Claim 25 recites a method, comprising "associating a user program key with a user program configured to run on a user data processor; . . . associating a machine key device with the particular user data processor, wherein the machine key device is accessible by the user program, and wherein the machine key device maintains a portion of a machine key; . . . encrypting the data object such that decryption of a first secure layer and a second secure layer of the encrypted data object requires the user program key and the machine key, respectively; . . . associating a user key device with the particular user, wherein the user key device is accessible by the user program, and wherein the user key device maintains a portion of a user key; and . . . encrypting the data object such that decryption of a third secure layer of the encrypted data object requires the user key."

Similarly, Claim 32 recites a method, comprising "associating a user program key with a user program configured to run on a user data processor; . . . encrypting the data object such that decryption of a first secure layer of the encrypted data object requires the user program key; . . . associating a machine key device with the particular user data processor, wherein the machine key device is accessible by the user program, and wherein the machine key device maintains a portion of a machine key for decrypting a second secure layer of the encrypted data object; . . . associating a user key device with the particular user, wherein the user key device is accessible by the user program, and wherein the user key device maintains a portion of a user key for decrypting a third secure layer of the encrypted data object."

Similarly, Claim 38 recites a method, comprising "associating a user program key with a user program configured to run on a user data processor; . . . associating a machine key with the particular user data processor; . . . decrypting a first secure layer and a second secure layer of the data object using the user program key and the machine key, respectively; . . . associating a user key with the particular user; . . . and . . . decrypting a third secure layer of the data object using the user key."

Similarly, Claim 44 recites "a secure data package . . . comprising a controlled portion of the data object, the controlled portion encrypted such that decryption of a first secure layer and a second secure layer of the encrypted data object requires both a user program key and a machine key, respectively, wherein a portion of the user program key is maintained by and associated with a user program configured to run on a user data processor to provide controlled access to the data object, wherein the user data processor has a permanently attached machine key device configured to maintain the machine key, and wherein the controlled portion comprises an essential portion of the data object, wherein the controlled portion is additionally encrypted such that decryption of a third secure layer of the encrypted data object requires a user key, wherein the user key is maintained by a user key device associated with a particular user and detachably connected to the processing device."

Therefore, because Sims in view of Abbott does not disclose or suggest all the limitations of independent Claims 1, 25, 32, 38, and 44, Claims 1, 25, 32, 38, and 44 are patentable over Sims in view of Abbott.

Claims 2-3, 5-7, 9, 12-17, 19-24, and 46-48 are dependent on Claim 1, Claims 26-29 and 31 are dependent on Claim 25, Claims 35-37 are dependent on Claim 32, Claims 40-43 are dependent on Claim 38, and contain additional limitations that further distinguish them from Sims in view of Abbott. Therefore, Claims 2-3, 5-7, 9, 12-17, 19-24, 26-29, 31, 35-37, 40-43, and 46-48 are patentable over Sims in view of Abbott for at least the same reasons stated above with regard to Claims 1, 25, 32, and 38.

Claim 18 is rejected under 35 U.S.C. § 103(a) as being unpatentable over Sims in view of Abbott and further in view of Keeler, Jr. et al. (U.S. Patent No. 6,502,130 hereinafter "Keeler"). Keeler is directed toward a "system and method which collects dynamic connectivity data from an area network interconnecting multiple computing devices" (Keeler, Abstract) and does not remedy the deficiencies of Sims and Abbott noted above. Claim 18 is also dependent on Claim 1 and contains additional limitations that further distinguish it from Sims in view of Abbott and further in view of Keeler. Therefore, because neither Sims nor Abbott nor Keeler, alone or in combination, disclose or suggest all the limitations of Claim 18, Claim 18 is patentable over Sims in view of Abbott and further in view of Keeler for at least the same reasons stated above with respect to Claim 1.

CONCLUSION

For the above reasons, Applicant believes pending Claims 1-3, 5-7, 9, 12-29, 31-32, 35-38, 40-44, and 46-48 are now in condition for allowance and allowance of the application is hereby solicited. If the Examiner has any questions or concerns, the Examiner is hereby requested to telephone Applicants' Attorney at (949) 752-7040.

Certificate of Transmission

I hereby certify that this correspondence is being facsimile transmitted to the Commissioner for Patents, Fax No. 703-872-9306 on the date stated below..

Tina

Tina Kavanaugh September 5, 2006

Respectfully submitted,

David A. Park

David S. Park
Attorney for Applicant(s)
Reg. No. 52,094